

SaTC: Small: Side-channel Attacks Against Mobile Users: Singularity Detection, Behavior Identification, and Automated Rectification

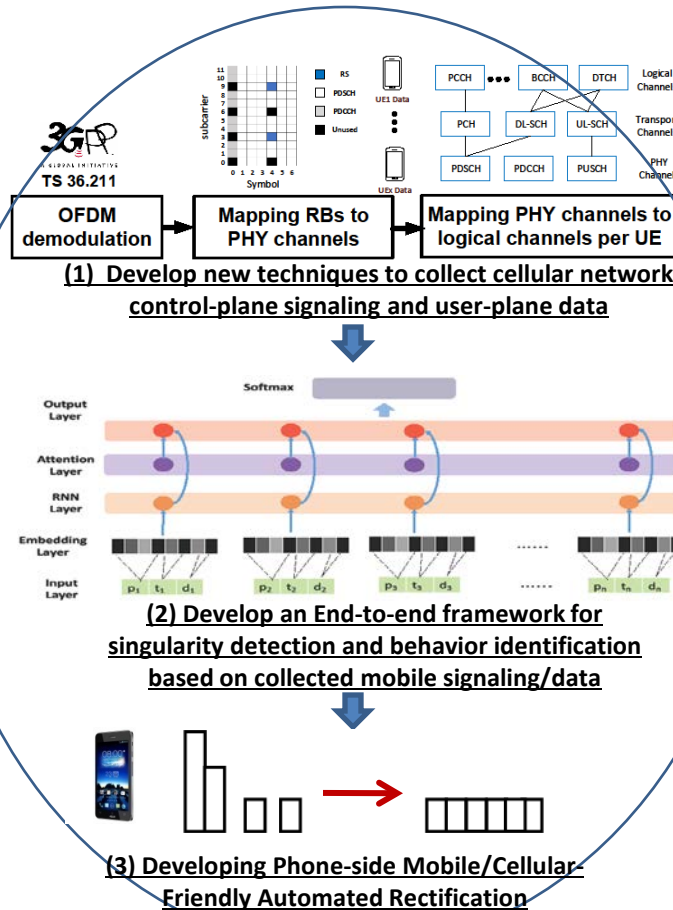


Challenge

- Detecting the singularity that can be used to identify mobile user and network behaviors is challenging in practice since (1) in cellular network, both cellular control-plane messages and user-plane data are encrypted and transmitted on the same physical channel; (2) typically the data is sequential and high-dimensional; (3) only limited labeled data is available; and (4) new behaviors can be emerging any time.
- The remedies against traffic-analysis-based side-channel attacks, such as padding packets, may not be practical since users have to pay for these extra data.

Solution:

- We leverage both cellular-domain knowledge and machine learning techniques to better recognize control-plane signaling and user-plane data from physical channels and label them with user behavior.
- On the top of labeled mobile data, we develop an end-to-end framework to detect the singularity that can infer user behavior.
- We develop phone-side cellular/mobile friendly automated rectification mechanisms to remove the singularity so that adversaries cannot launch the side-channel attacks.



Scientific Impact:

- This project extends the state-of-the-art side-channel attack research to a new frontier of mobile networks, investigates original problems that entreat innovative solutions, and paves the way for a new research endeavor to tame diversified traffic for discovering insightful singularities.
- This project will develop new tools for mobile data collection and labeling, novel algorithms for singularity detection and behavior identification, and original techniques to mitigate the real-world attack damage.

Broader Impact:

- The lessons learned from this proposal can also provide new insights for the security design of the 5G networks.
- This project allows the PI/Co-PI to integrate the research results into both undergraduate and graduate curricula, which will expose CS students to interdisciplinary research. This project will contribute to the nation's workforce with students that are well trained in mobile systems, wireless networking, and data science.

Project number: CNS-1815636

Leading institution: Michigan State University

Contacts: Guan-Hua Tu (gthu@msu.edu);

Jiliang Tang (tangjili@msu.edu).